

UNITED STATES DISTRICT COURT

for the
Northern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
SEE ATTACHMENT A

Case No. 3:18-MJ-469 (TWD)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

Evidence of transporting, distributing, receiving or possessing child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A, as more particularly described in attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code, Sections 2252 and 2252A	Transportation, Distribution, Receiving or Possession of Child Pornography


The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ATTESTED TO BY THE APPLICANT IN
ACCORDANCE WITH THE REQUIREMENTS OF
RULE 4.1 OF THE FEDERAL RULES OF
CRIMINAL PROCEDURE

 Applicant's signature
 Jenelle Corrine Bringuel, Special Agent

Sworn to before me and signed in my presence.

Date: 08/17/2018City and state: Syracuse, New York

 Judge's signature
 Hon. Thérèse Wiley Dancks
 Printed name and title

ATTACHMENT A

PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) 68 Quinn Hill Road, Port Crane, NY 13833, (B) the persons of Larissa Hiller and Jack G. Hiller Jr., (C) a 2016 GMC Sierra Pick-up truck, blue in color, VIN# 1GTV2MEC5GZ305090, NY Registration: FFP2664, registered to Jack G. Hiller Jr, (D) a 2016 Chevrolet Malibu, four-door-sedan, tan in color, VIN# 1G11C5SA5GF129740, NY Registration: FJW3219, registered to Jack G. Hiller Jr, (E) a 2012 Chevrolet Equinox, SUV, red in color, VIN# 2GNALDEK7C6247922, NY Registration: FWJ4647, registered to Jack G. Hiller Jr, (F) a 2018 Image Boat Co. House Trailer, white in color, VIN# 573TE3021J6609509, NY Registration: BP15633, registered to Jack G. Hiller Jr, and (G) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches.

The residence at 68 Quinn Hill Road, Port Crane, NY is a one story single family house with blue siding and white shutters situated on the eastern shoulder of Quinn Hill Road. Directly south of the residence is a detached two car garage with the same blue colored siding and a white side door facing Quinn Road. There is a sidewalk that leads from the western side of the garage to a wooden deck on the front of the residence. On this wooden deck is a white door on the western side of the house facing Quinn Hill Road. A driveway runs westward from the detached garage to Quinn Hill Road. At the end of the driveway there is a black mailbox with "68" numbered on it in metallic colored numbers. Next to the mailbox is a blue fire number sign with "68" numbered in white.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items of evidence in violation of Title 18 USC §§ 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography):

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.
6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies);

any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored or maintained), books, notes, and reference materials.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use, including the use of Kik Messenger, username "Jumpin Jack," and/or "jumpinjack72," and e-mail wagnfoxisl@yahoo.com.

11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.

12. Documents and records, in any form or format, regarding the identity of any person using Kik Messenger, P2P file sharing software, and the use of any other methods of receiving, transporting, or distributing images of children engaged in sexually explicit conduct.

13. Documents and records regarding the ownership and/or possession of the searched premises.

14. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

Materials Relating to Child Erotica and Depictions of Minors

15. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.
16. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.
17. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).
18. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.
19. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

Photographs of Search

20. During the course of the search, photographs of the searched premises and vehicles may also be taken to record the condition thereof and/or the location of items therein.

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK**

**IN THE MATTER OF AN APPLICATION
OF THE UNITED STATES OF AMERICA
FOR SEARCH WARRANTS FOR:**

[SEE ATTACHMENT A-B, HEREIN]

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

JENELLE CORRINE BRINGUEL, being duly sworn, deposes and states:

INTRODUCTION

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI since June of 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I am investigating the activities of the IP addresses 50.108.196.118, 172.79.144.241, and 50.108.194.14 all subscribed to by Larissa Hiller, who resides at 68 Quinn Hill Road, Port Crane, NY 13833 (the Subject Premises, as more fully described in Attachment A). As will be shown below, there is probable cause to believe that someone using the IP addresses registered to Larissa Hiller at the Subject Premises, has transported, received, possessed, or distributed child pornography, in violation of 18 U.S.C.

§§ 2252 and 2252A, and I submit this application and affidavit in support of search warrants authorizing a search of (A) 68 Quinn Hill Road, Port Crane, NY 13833, (B) the persons of Larissa Hiller and Jack G. Hiller Jr, (C) a 2016 GMC Sierra Pick-up truck, blue in color, VIN# 1GTV2MEC5GZ305090, NY Registration: FFP2664, registered to Jack G. Hiller Jr, (D) a 2016 Chevrolet Malibu, four-door-sedan, tan in color, VIN# 1G11C5SA5GF129740, NY Registration: FJW3219, registered to Jack G. Hiller Jr, (E) a 2012 Chevrolet Equinox, SUV, red in color, VIN# 2GNALDEK7C6247922, NY Registration: FWJ4647, registered to Jack G. Hiller Jr, (F) a 2018 Image Boat Co. House Trailer, white in color, VIN# 573TE3021J6609509, NY Registration: BP15633, registered to Jack G. Hiller Jr, and (G) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches. Located within the places and items to be searched, I seek to seize evidence, fruits, and instrumentalities of criminal violations relating to the knowing transportation, shipment, receipt, possession, and distribution, of child pornography, as more particularly described in Attachment B.

4. As will be demonstrated in this affidavit, made under Fed. R. Crim. P. Rule 41, there is probable cause to believe that evidence will be located at the Subject Premises, on the persons of Larissa Hiller and Jack G. Hiller Jr, in the vehicles registered to Jack G. Hiller Jr, and within computers, computer equipment and/or other electronic media relating to violations of Title 18, United States Code 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography), hereafter referred to as the Subject Offenses.

5. The statements and facts set forth in this affidavit are based in significant part on: my review of written documents obtained from the FBI Albany Child Exploitation Task Force, my review of written documents obtained from the FBI Washington Field Office Child Exploitation and Human Trafficking Task Force, conversations and review of documents obtained by Mid-State Child Exploitation Task Force Officer and NYSP Investigator Joshua Kresge, and my personal training and experiences. Since this Affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts

and circumstances that I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A are presently located within the places and items to be searched.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

6. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, your Affiant knows that electronic devices, including computers and cellular telephones, serve different roles or functions with child pornography: production, communication, distribution, and storage.

7. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within recent years. These drives can store thousands of images at very high resolution.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user

can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

11. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

COLLECTORS OF CHILD PORNOGRAPHY

12. Individuals who are interested in child pornography may want to keep the child pornography files they receive for use in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy and security of their homes or other secure location. Additionally, individuals who utilize social media are known to keep their electronic media with them, including at their homes.

13. Individuals who collect child pornography may seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not

limited to, mail, email groups, bulletin boards, IRC, newsgroups, instant messaging, Peer to peer programs, and other similar vehicles.

14. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

15. Individuals who collect child pornography may keep names, e-mail addresses, phone numbers or lists of persons who have shared, advertised or otherwise made known their interest in child pornography or sexual activity with children. These contacts may be maintained as a means of personal referral, exchange or commercial profit. This information may be maintained in the original medium from which it was derived, in lists, telephone or address, on computer storage devices, or merely on paper.

BACKGROUND OF THE INVESTIGATION

16. On February 20, 2018 the FBI Washington Field Office (WFO) was alerted by the FBI Detroit Division that a subject, M.M., while using the “Kik” app under the username of “MGMFREEDOM,” exchanged child pornography images with multiple Kik app users, to include a subject, B.K., of Marysville, Michigan. On February 21, 2018, M.M. was interviewed by FBI WFO and admitted to taking pornographic images of his 8-year-old step-daughter and sending them to other users on the Kik app. Forensic analysis of M.M.’s devices determined that M.M. exchanged child pornography images and/or videos with Kik user, “jumpinjack72,” from January 27, 2018 to February 26, 2018.

17. On May 22, 2018, TFO Kresge viewed the Kik chats and images exchanged between “mgmfreedom” and “jumpinjack72.” Conversations between “mgmfreedom” and “jumpinjack72” start on February 2, 2018, in which “jumpinjack72” states that he lost stuff and “mgmfreedom” asks him what

he likes. The Kik user “jumpinjack72” advises that he likes teens, bi, and bbw¹ as well as young. A review of the Kik messages between “mgmfreedom” and “jumpinjack72” showed “mgmfreedom” distributed numerous images of child pornography to “jumpinjack72” including three images of nude females between the ages of 5 and 10 years old who were tied up and bound by the hands and feet, three of which are described as follows:

- a. On February 2, 2018 at 9:59 PM, “mgmfreedom” sent “jumpinjack72” a file named “4c39a62a-d689-4e81-ad08-ff1fdb0bfe8a” which contains a teen female orally licking the naked genitals of a pre-pubescent female approximately 6-10 years in age.
- b. On February 3, 2018 at 9:17 AM, “mgmfreedom” sent “jumpinjack72” a file named “d906e9a5-3a4b-408e-ab10-99ffa7ec7951.jpg” which depicts an adult male standing and having vaginal sexual intercourse with nude female approximately 6-10 years in age who is laying on her back.
- c. On February 3, 2018 at 9:31 AM, “mgmfreedom” sent “jumpinjack72” a file named “dd1c9eec-37b9-4c6a-8a6a-e528babea8e3.jpg” which depicts a nude male approximately 6-10 years old kneeling in front of a standing adult male and the adult male’s penis in the 6-10 year old male’s mouth.

18. The Kik user “jumpinjack72” is associated with e-mail address of wagnfoxisl@yahoo.com, a mobile telephone number of 607-760-9160, and several login IP addresses: 50.108.196.118, 172.79.144.241, and 50.108.194.14, which are associated with Jack and Larissa Hiller of 68 Quinn Hill Road, Port Crane, NY 13833:

- a. On February 26, 2018, an administrative subpoena was issued to and served on Kik requesting subscriber identification information and IP access logs associated with the “jumpinjack72” account. Kik responded to the subpoena and provided a display name of “Jumpin Jack”, and an e-mail of wagnfoxisl@yahoo.com for the username “jumpinjack72.” Kik also provided IP logs from January 27, 2018 to February 26, 2018,

¹ “Bi” refers to “bisexual” and “bbw” refers to “big beautiful women.”

that showed several Frontier Communications IP addresses (50.108.196.118, 172.79.144.241, and 50.108.194.14) regularly being used to access the “jumpinjack72” account during this time period.

b. On February 26, 2018, an administrative subpoena was issued to and served on Frontier Communications requesting the subscriber name, address of service, and billing information associated with IP addresses 50.108.196.118 on 01/27/18 at 14:45:13 UTC and 172.79.144.241 on 01/29/18 at 17:24:53 UTC, which were the first times those IP addresses appeared in the administrative subpoena results received from Kik, and 50.108.194.14 on 02/26/18 at 09:26:53 UTC, which was the most recent login to the Kik account at the time the information was received by your Affiant from FBI WFO. Frontier responded that on those dates and times each of the IP addresses were assigned to the account at 68 Quinn Hill Road, Port Crane, NY 13833, under the customer name Larissa Hiller, with an associated e-mail address of jacnris1992@frontier.com. Service to that subscriber at that location was activated on 11/09/2009.

c. An administrative subpoena was issued to and served on Yahoo! Requesting subscriber identification information for the e-mail address of wagnfoxisl@yahoo.com. Yahoo! responded with a subscriber name of Jack Ris, created on 04/28/2015, with a telephone number of 607-760-9160.

d. An administrative subpoena was issued to and served on Verizon Wireless requesting subscriber identification information for the mobile telephone number of 607-760-9160. Verizon Wireless responded with a subscriber name of Jack and Larissa Hiller, an address of 68 Quinn Hill Road, Port Crane, NY 13833, and an e-mail address of jacnris1992@frontier.com.

19. On May 8, 2018, TFO Kresge conducted physical surveillance of 68 Quinn Hill Road, Port Crane, NY and secured a photograph of the residence. This photograph of 68 Quinn Hill Road, Port Crane, NY is contained in Attachment A.

20. The residence at 68 Quinn Hill Road, Port Crane, NY is a one story single family house with blue siding and white shutters situated on the eastern shoulder of Quinn Hill Road. Directly south of the residence is a detached two-car garage with the same blue colored siding and a white side door facing Quinn Road. There is a sidewalk that leads from the western side of the garage to a wooden deck on the front of the residence. On this wooden deck is a white door on the western side of the house facing Quinn Hill Road. A driveway runs westward from the detached garage to Quinn Hill Road. At the end of the driveway there is a black mailbox with "68" numbered on it in metallic colored numbers. Next to the mailbox is a blue fire number sign with "68" numbered in white.

21. On May 9, 2018, TFO Kresge conducted New York State DMV registration checks for Jack G. Hiller Jr. and Larissa A. Hiller of 68 Quinn Hill Road, Port Crane, NY 13833. The following vehicles, all of which have been observed at the residence during physical surveillance, are currently registered to Jack G. Hiller Jr at the Subject Premises:

a. A 2018 Image Boat Co. House Trailer, white in color, VIN# 573TE3021J6609509, NY
Registration: BP15633

b. A 2016 GMC Sierra Pick-up truck, blue in color, VIN# 1GTV2MEC5GZ305090, NY
Registration: FFP2664

c. A 2016 Chevrolet Malibu, four-door-sedan, tan in color, VIN# 1G11C5SA5GF129740, NY
Registration: FJW3219

d. A 2012 Chevrolet Equinox, SUV, red in color, VIN# 2GNALDEK7C6247922, NY
Registration: FWJ4647

22. On 8/8/2018, just prior to 6 a.m., TFO Kresge observed Jack G. Hiller Jr. driving the 2012 Chevrolet Equinox, SUV, registered to him at the Subject Premises, driving down Bally Hack Road, Port Crane, NY toward New York State Route 369. TFO Kresge followed Hiller to a New York State Department of Transportation (DOT) facility a short distance from his residence. TFO Kresge observed Hiller park his vehicle, exit the vehicle, and enter the DOT facility at approximately 6:02 a.m. Prior to

this date, TFO Kresge conducted NY State Police database searches and observed that Hiller was employed by New York DOT. On that same date, TFO Kresge observed Jack G. Hiller Jr. departing the DOT facility at 2:33 p.m. Hiller returned to the Subject Premises at approximately 2:38 p.m. in the 2012 Chevrolet Equinox, SUV, which he parked in the garage of the Subject Premises. As your Affiant believes Jack G. Hiller Jr. departs the residence for work several minutes prior to 6:00 a.m., your Affiant intends to execute the warrant prior to 6:00 a.m., but not prior to 5:00 a.m., because it is believed Hiller will be awake at that time. As the requested search warrant includes a search of Hiller's person as well as all vehicles registered to him, it is important to execute the search warrant while Hiller is present at the house because if Hiller learns that a search is ongoing at the residence while he is not there he might destroy any evidence on his person or in the vehicle he takes to work.

23. On 8/9/2018, the United States Postal Inspection Service provided that the following individuals receive mail at the Subject Premises: Jack Hiller Sr., Jack Hiller Jr., Larissa Hiller, and Ashley Hiller.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. Your Affiant has spoken with law enforcement personnel trained in computer evidence recovery who have knowledge about the operation of computer systems and the correct procedures for the seizure and analysis of computer systems.

25. These individuals have participated in the execution of numerous search warrants during which they have seized and/or examined computer systems. These individuals have also participated in several warrants that involved the search and/or seizure of, and has been responsible for analyzing, seized electronic data and records from those systems.

26. Based on my experience and training, plus the common sense knowledge that in today's technological world, computers and computer related media are used for communication and storage of data and information. As such, it is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format.

27. Furthermore, based upon my training, experience, and consultations with law enforcement personnel who specialize in searching computer systems, your Affiant has learned that searching and seizing information from computer systems and other storage media (including PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

28. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in mere desktop computers are capable of storing millions of pages of text; the storage capacity of other electronic devices (e.g. a micro drive, a thumb drive, etc.) can also be significant. Unlike the search of documentary files, computers store data in "files" that cannot easily be reviewed. For instance, a single 1 gigabyte of storage media is the electronic equivalent of approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

29. The search through the computer (or other electronic media) itself is a time consuming process. Software and individual files can be "password protected." Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names ("Smith.ltr") can in fact be electronic commands to electronically cause the data to self-destruct. Also, files can be "deleted," but, unlike documents that are destroyed, the information and data from "deleted" electronic files usually remains on the storage device until it is "over written" by the computer. For example, the computer's hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non-deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the

“pointers” have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the “deleted” file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time-consuming procedure to review the contents of the computer storage device so as to insure the integrity of the data and/or evidence. A single computer and related equipment could take many days to analyze properly.

30. Computer storage media are used to save copies of files and communications, and printers are used to make paper copies of these communications and files. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. All these parts of a computer are integrated into the entire operation of a computer. In order to evaluate the evidence most effectively, the computers and all of the related computer equipment described above should be available to a computer investigator/analyst.

31. Therefore, based upon my knowledge, training, and experience, as well as information related to me by Special Agents and others involved in forensic examination of computers, your Affiant is aware that searches for and seizures of evidence from computers commonly require Agents to seize most or all of a computer system’s input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit.

32. Furthermore, searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

33. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

34. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

35. Based upon my training and experience and conversations with other law enforcement personnel, your Affiant is aware that a number of computer storage devices are quite small and portable, and can be easily hidden on a person. For instance, digital cameras can store numerous digital images on a disk approximately the size of a postage stamp. In addition, thumb drives, which are approximately the size of a pocket knife, can hold numerous images and computer videos. Your Affiant also knows, from my training and experience, that these devices are often stored in vehicles to prevent other users in the home from discovering the existence of the child pornography collection. Your Affiant, therefore, also requests permission to search the persons of Larissa Hiller and Jack G. Hiller Jr., and the vehicles registered to Jack Hiller, for such evidence.

SEARCH METHODOLOGY TO BE EMPLOYED

36. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a) on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b) examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c) searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d) surveying various file directories and the individual files they contain;

e) opening files in order to determine their contents;

f) scanning storage areas;

g) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h) performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

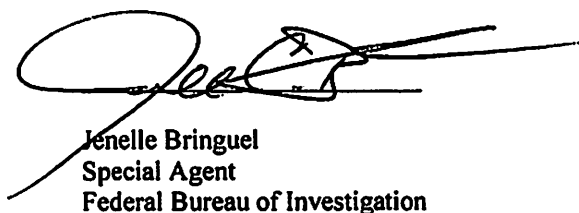
CONCLUSION

37. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that someone using IP addresses of 50.108.196.118, 172.79.144.241, and 50.108.194.14 at a time each were assigned to the account subscribed to by Larissa and Jack G. Hiller Jr, at the Subject Premises, is involved in the transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A, is located in the Subject Premises, on the persons of Larissa Hiller and Jack G. Hiller Jr, in the vehicles registered to

Jack G. Hiller Jr, and within computers, computer equipment and/or other electronic media located therein or within the Subject Kik Account.

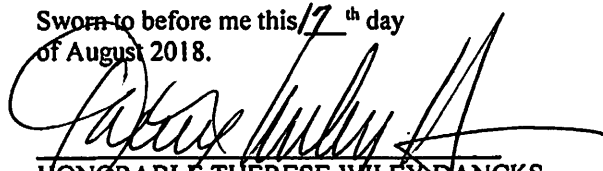
38. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of (A) 68 Quinn Hill Road, Port Crane, NY 13833, (B) the persons of Larissa Hiller and Jack G. Hiller Jr., (C) a 2016 GMC Sierra Pick-up truck, blue in color, VIN# 1GTV2MEC5GZ305090, NY Registration: FFP2664, registered to Jack G. Hiller Jr, (D) a 2016 Chevrolet Malibu, four-door-sedan, tan in color, VIN# 1G11C5SA5GF129740, NY Registration: FJW3219, registered to Jack G. Hiller Jr, (E) a 2012 Chevrolet Equinox, SUV, red in color, VIN# 2GNALDEK7C6247922, NY Registration: FWJ4647, registered to Jack G. Hiller Jr, (F) a 2018 Image Boat Co. House Trailer, white in color, VIN# 573TE3021J6609509, NY Registration: BP15633, registered to Jack G. Hiller Jr, and (G) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE.



Jenelle Bringuel
Special Agent
Federal Bureau of Investigation

Sworn to before me this 7th day
of August 2018.



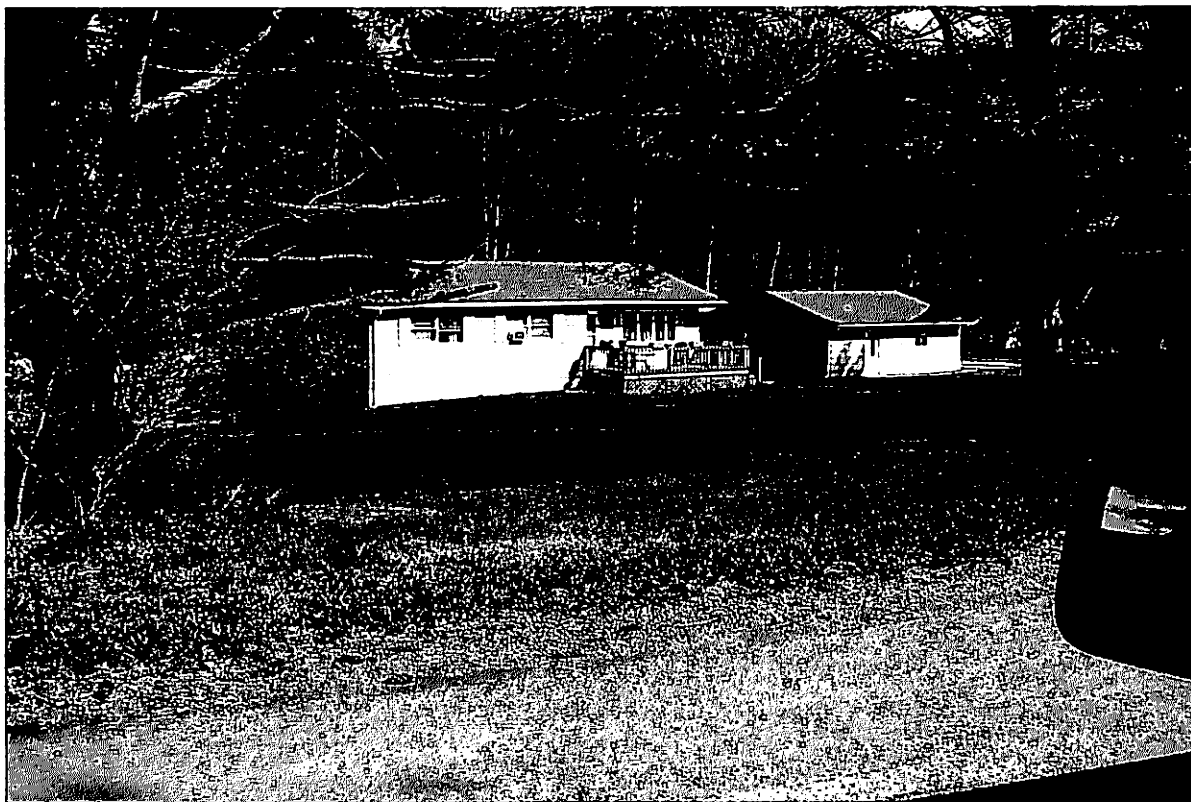
HONORABLE THERESE WILEY DANCKS
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A

PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) 68 Quinn Hill Road, Port Crane, NY 13833, (B) the persons of Larissa Hiller and Jack G. Hiller Jr., (C) a 2016 GMC Sierra Pick-up truck, blue in color, VIN# 1GTV2MEC5GZ305090, NY Registration: FFP2664, registered to Jack G. Hiller Jr, (D) a 2016 Chevrolet Malibu, four-door-sedan, tan in color, VIN# 1G11C5SA5GF129740, NY Registration: FJW3219, registered to Jack G. Hiller Jr, (E) a 2012 Chevrolet Equinox, SUV, red in color, VIN# 2GNALDEK7C6247922, NY Registration: FWJ4647, registered to Jack G. Hiller Jr, (F) a 2018 Image Boat Co. House Trailer, white in color, VIN# 573TE3021J6609509, NY Registration: BP15633, registered to Jack G. Hiller Jr, and (G) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches.

The residence at 68 Quinn Hill Road, Port Crane, NY is a one story single family house with blue siding and white shutters situated on the eastern shoulder of Quinn Hill Road. Directly south of the residence is a detached two car garage with the same blue colored siding and a white side door facing Quinn Road. There is a sidewalk that leads from the western side of the garage to a wooden deck on the front of the residence. On this wooden deck is a white door on the western side of the house facing Quinn Hill Road. A driveway runs westward from the detached garage to Quinn Hill Road. At the end of the driveway there is a black mailbox with "68" numbered on it in metallic colored numbers. Next to the mailbox is a blue fire number sign with "68" numbered in white.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items of evidence in violation of Title 18 USC §§ 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography):

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.
6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies);

any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored or maintained), books, notes, and reference materials.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use, including the use of Kik Messenger, username "Jumpin Jack," and/or "jumpinjack72," and e-mail wagnfoxisl@yahoo.com.

11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.

12. Documents and records, in any form or format, regarding the identity of any person using Kik Messenger, P2P file sharing software, and the use of any other methods of receiving, transporting, or distributing images of children engaged in sexually explicit conduct.

13. Documents and records regarding the ownership and/or possession of the searched premises.

14. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

Materials Relating to Child Erotica and Depictions of Minors

15. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.

16. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

17. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).

18. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.

19. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

Photographs of Search

20. During the course of the search, photographs of the searched premises and vehicles may also be taken to record the condition thereof and/or the location of items therein.